Cybersecurity

Cybersecurity Initiatives

The Bank is strengthening its cybersecurity measures as it recognizes the threat of increasingly sophisticated and intricate cyberattacks as an important managerial risk.

Basic Policy on Cybersecurity

The Bank has established a basic policy for cybersecurity management in the "Basic Regulations on Cyber Security" to minimize the risk of cyber incidents causing damage to the Bank's customers and/or disrupting the Bank's operations or the financial system as a whole.

Cybersecurity Structure

As for organizational structure, we designate the Director in charge of the IT & Systems Planning Division as the "Chief Information Officer" to clarify roles and responsibilities regarding cyber risks. Under the supervision of the Chief Cyber Security Officer, various measures are in place, led by the IT & Systems Planning Division in charge of cybersecurity.

The occurrence of cyber incidents, threat trends and the status of cybersecurity measures in place are regularly reported to the Board of Directors and other management-level meetings such as the Business Infrastructure Committee and the Operational Risk Management Committee, where cybersecurity policies are discussed.

Within the IT & Systems Planning Division is a team specializing in cybersecurity called the "Computer Security Incident Response Team (CSIRT)." The Bank's CSIRT works closely with the SOC, or Security Operation Center, which is staffed by an external security vendor, and monitors events that could be signs of a cyber incident 24 hours a day, 365 days a year, thereby preparing for an initial response when a cyber incident occurs. The CSIRT also collaborates with the government, law enforcement agencies and various organizations such as ISAC to gather information on cyberattack tactics and new vulnerabilities and to strengthen countermeasures.

Furthermore, to ensure cyber resilience, the Bank established procedures and contingency plans for responding to cyber incidents and confirm the roles and procedures of each department through periodic incident response exercises.

Cybersecurity Management Process

Regarding the confidentiality, integrity and availability of its information systems, the Bank assesses system risks, based on the "Security Guidelines on Computer Systems for Banking and Related Financial Institutions" and other information from the Center for Financial Industry Information Systems ("FISC"), and implements necessary control measures.

As a cross-organizational cybersecurity management process, the Bank organizes "cybersecurity programs" in accordance with NIST's Cybersecurity Framework from the perspectives of "identify," "protect," "detect," "respond" and "recover," and reviews necessary measures based on external threats such as changes in attackers' tactics and internal vulnerabilities.

The effectiveness of these cybersecurity management efforts is confirmed through internal and external audits, as well as vulnerability assessments and penetration tests.

Education on Cybersecurity

The Bank provides education for different purposes to improve the knowledge and awareness required of each of its directors and employees.

- E-learning for the Bank's directors and employees to acquire basic knowledge of security
- Newsletters for presenting cybersecurity-related articles to raise awareness of cybersecurity among the Bank's directors and employees
- Suspicious e-mail trainings for all directors and employees to increase their awareness of and readiness for targeted e-mail attacks
- Lectures by experts to improve the knowledge on cybersecurity of directors
- Incident response trainings for directors and staff of relevant departments to confirm response procedures in the event of a cyber incident
- Trainings by external experts to improve CSIRT's forensic skills

The Bank also established an external qualification incentive program to develop cybersecurity specialists and improve their professional skills.